IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
SAN ANTONIO DIVISION

MELODY JOY CANTU AND DR. RODRIGO CANTU,	§	
Plaintiffs,	§	
V.	§	CIVIL ACTION NO. 5:20-CV-0746-JKP
DR. SANDRA GUERRA and DIGITAL FORENSICS CORPORATION, LLC,	§	
Defendants.	§	

DEFENDANT DIGITAL FORENSICS CORPORATION, LLC
DESIGNATION OF EXPERT WITNESSES

TO THE HONORABLE UNITED STATES DISTRICT JUDGE:

Defendant Digital Forensics Corporation, LLC ("Defendant") submits the following expert witness disclosures:

I.

Pursuant to Fed. R. Civ. P. 26(a)(2) and Local Rule CV-26(b), Defendant designates the following witnesses it may use at trial to present evidence under Federal Rule of Evidence 702, 703, or 705:

1. Shawn Kasal
12 Points Technologies, LLC
Cyber Security & Forensics
3738 South 149th Street
Suite 116
Omaha, NE 68144

Mr. Kasal is a digital forensic expert. Attached hereto as Exhibits "A" and "B" respectively, is a copy of Mr. Kasal's expert report and resume. Defendant reserves the right to amend and/or supplement this designation as discovery continues and is completed.

2. J. David Apple
Apple & Fink, LLP

735 Plaza Blvd., Suite 200
Coppell, Texas 75019
(972) 315-1900

Mr. Apple is an attorney licensed to practice law in the State of Texas. He was admitted to practice law in the State of Texas in 1990, and has been engaged in the practice of law continuously since that time. Mr. Apple's practice has been principally devoted to civil litigation. Mr. Apple is the senior litigation and managing partner in the law firm Apple & Fink, LLP. He has spent his entire legal career representing clients in various litigation matters across Texas and other states. Mr. Apple is familiar with the reasonable and customary fees charged by attorneys in Texas for cases of this nature. Mr. Apple has also been qualified and testified as an expert witness on attorneys' fees in a number of different courts during his career.

Mr. Apple is expected to testify concerning the attorneys' fees, costs, and expenses incurred by Defendant in this suit, including the cost for any and all appeals. His impressions and opinions are based upon his knowledge of the work performed by the attorneys and paralegals at Apple & Fink, LLP, as well as Defendant's prior attorneys. He is expected to testify that the fees and costs charged by Defendant's attorneys are reasonable and necessary for this type of case. The basis for the opinions will be related to the work done in the case, the hourly fees charged for such services, and the experience of the attorneys who are litigating this case. The amount of attorneys' fees is ongoing and will increase through trial. Mr. Apple is also expected to testify concerning the attorneys' fees, costs, and expenses incurred by Plaintiffs in this suit, including the cost for any and all appeals. His impressions and opinions will be based upon his review of the fee statements reflecting the work performed by the attorneys and paralegals at those law firms representing Plaintiffs.

Mr. Apple will testify that the fees incurred through trial by Apple & Fink, LLP are reasonable and necessary, and are consistent with those fees customarily charged by other law firms in similar cases. Mr. Apple will testify that $450.00 is a reasonable hourly rate for his services and the services of any other attorney assisting with the trial, $100-$175 is a reasonable hourly rate for his legal assistants, and that these hourly rates are well within the range customarily charged by attorneys and legal assistants with similar experience in the Western District of Texas.

Mr. Apple will also base his impressions and opinions on those factors set forth in Rule 1.04 of the Texas State Bar Rules which include, but are not limited to, the time and labor required, the novelty and difficulty of the questions involved, the skill required to perform the legal services properly, and the fee customarily charged in the locality for similar legal services.

All time records representing or regarding the attorneys' fees incurred herein by Defendant will be produced in redacted form before trial along with a current copy of Mr. Apple's resume which can be found at www.applefinklaw.com.

II.

Defendant reserves the right to call, examine and elicit opinions from any person designated by the other parties as an "expert" in this case.

Respectfully submitted,

By: /s/ J. David Apple
J. David Apple
State Bar No. 01278850

APPLE & FINK, L.L.P.
735 Plaza Blvd., Suite 200
Coppell, Texas 75019
Telephone: (972) 315-1900
Facsimile: (972) 315-1955
Email: jdapple@applefinklaw.com

ATTORNEYS FOR DEFENDANT DIGITAL FORENSICS CORPORATION, LLC

CERTIFICATE OF SERVICE

I hereby certify that on November 8, 2021, I electronically filed the foregoing document with the Clerk of the Court for the United States District Court, Western District of Texas, San Antonio Division, using the electronic case filing system of the court, which will send a "Notice of Electronic Filing" to the following counsel:

Tor Ekeland
Tor Ekeland Law, PLLC
195 Montague Street, 14th Floor
Brooklyn, NY 11201
tor@torekeland.com

Rain Levy Minns
Minns Law Firm, P.C.
d/b/a Rain Minns Law Firm
4412 Spicewood Springs Road, Suite 500
Austin, Texas 78759
rain@rainminnslaw.com

Ricardo G. Cedillo
Brandy C. Perry
Davis, Cedillo & Mendoza, Inc.
755 E. Mulberry, Suite 250
San Antonio, Texas 78212
rcedillo@lawdcm.com
bperry@lawdcm.com

/s/ J. David Apple
J. David Apple

EXHIBIT A

Your Digital Shadow

My name is Shawn Kasal and I am a digital forensics expert. I've had the opportunity to serve and be qualified as a forensic expert in Nebraska state district and federal court. I have testified in courts across the United States. My CV is attached. I was retained by legal counsel, Jeromy Simonovic, Esq. In-House Counsel Digital Forensics Corp to assist in their investigation of certain allegations regarding concerning online behavior.

Access to the internet at high speed has been generally available for over twenty years. Using the service in a familiar, private environment, people tend to feel they enjoy the same degree of seclusion in their online activities that they do in their own home. Nothing could be further from the truth.

Internet Structure and Administration:

When you access the internet in the United States you are almost certainly doing so via an IPv4 address that your internet service provider obtained from ARIN, the American Registry of Internet Numbers[1]. There are roughly four billion addresses in total, but they're doled out in blocks that are multiples of 256 addresses. Each active block is assigned to a service provider who pays for that privilege, who provides ARIN with business contact information, and who must respond to both subpoenas and search warrants. Each service provider is also required to comply with the terms of CALEA, the Communications Assistance for Law Enforcement Act[2]. This requires that the provider support traffic capture within their network in support of search warrants.

This original space of four billion addresses is fragmented due to administrative and technical concerns, with far less than 100% utilization. This was recognized as a problem a few years after the commercialization of the internet in the 1990s and by the turn of the century connecting via the IPv6 protocol became possible. The four billion addresses of the 32 bit IPv4 standard are slowly giving way to the enormous address space of 128 bit IPv6. Client and server software lags behind the protocol itself and given that the United States is the origin of the internet, we have a privileged position in regards to IPv4. This new protocol is something one would expect to see in industrialized Asia or developing markets, and it's more likely found on mobile devices that servers. There are four other global number registries, Europe's RIPE, Asia's APNIC, Central and South America's LACNIC, and AfriNIC. The rules regarding identifying the ISP associated with a given address block are fairly harmonious.

Domain Names and Resolution:

Every web site on the internet has a domain name. These names are purchased through registrars and the owner's name may be concealed by what is called a proxy registration[3]. Subpoenas and search warrants can unmask most domain operators. Barriers to identifying operators are numerous and proliferating, hence the qualification "most". Europe's General Data Protection Regulation functionally disappeared historic data on web sites associated with the continent. Proxy registration providers have a variety of uncooperative jurisdictions where they can base their business. The British Virgin Islands

---

[1]https://www.arin.net/resources/

[2]https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

[3]https://www.icann.org/resources/pages/privacy-proxy-registration-2013-03-22-en

and Panama are well known for their concealment, and those who work regularly in the area will run across names like Kazakhstan and Kyrgyzstan during investigations.
Once a domain name has been secured web sites are made accessible on the internet by configuring DNS, the Domain Name Service. The registrar is configured with the names of two or more DNS servers, and this information is distributed to thirteen global DNS root servers[4], enumerated as A through M. These systems are subject to intense interest by bad actors and they are globally distributed using anycast addressing. There are just thirteen names but there about about eleven hundred systems that answer requests.

The root servers do not know the particulars of every domain on the internet. Their role is to provide a pointer to the second tier DNS server at an internet service provider or hosting facility, which can then resolve the particulars about the domain.

When an internet service subscriber wishes to access a domain there is a three step name resolution process. The subscribers computer gives the name it wishes to access to a resolver, a type of DNS server that exists to make requests and cache the results. The resolver asks a root DNS server for the authoritative DNS servers for the domain in question. Once the resolver has this, it contacts the hosting DNS server and makes its request.

DNS resolution is the first step to any online misbehavior and there are many vendors who provide various security services to commercial internet clients and service providers. As a component of these services, the client agrees to permit harvesting of the DNS requests[5] originating from their network. Large providers of this service such as Farsight or RiskIQ can see 99.99% of the global DNS name space and they track the IP addresses of the hosts associated with each name, offering visibility that includes filtering based on activity time.

Tracking Web Clients:

Web sites are accessed by web browsers and each has a unique "fingerprint". The very first thing a web site learns about a visitor is the IP address from which they originate. The browser type, the version of software, and the screen resolution are all pieces of information that are available to the web site operator. This is used to make the site "responsive" – providing a smooth interaction no matter if the visitor is on a desktop computer or using a cell phone. Even the most basic of web servers log the date and time, IP address, and browser specifications for incoming requests.

There is a sprawling sector of the information economy that is dedicated to digging deeper into the relationship between a web site and its visitors. The motivations are varied, ranging from offering web developers a "customer's eye view" of how a site is performing to illuminating general demographics about visitors. The far end of this spectrum includes services ranging from tracking the latest model iPhones that visit from specific companies in order to offer highly targeted advertising to executives to the ability to delivery a personalized birthday greeting via a Facebook ad, having it appear just once for the intended recipient.

Web sites seeking to monetize their flow of visitors will almost always start by running Google Analytics, which provides tools to explore the nature of those who view the site.. As mentioned above, the first and most fundamental thing a web server knows about a visitors is their origin IP address.

---

[4]https://www.iana.org/domains/root/servers
[5]https://securitytrails.com/blog/passive-dns

There is an endless bazaar of options to look deeper. Some big names include Clicktale, Criteo, Demdex, Drift, Crowd Control, Hotjar, Kampyle, Kinja – there are about 200 that one must block using a browser extension in order to achieve a modicum of privacy.

Like the passive observation of DNS described above, web browser clients get the same level of attention from ad exchanges, audience understanding tools, consumer behavior analysis suites, and security vendors trying to spot intruders among potential customers. Some of these are free and the creators of these tools place a great value on synergy. The web site owner receives a service from which they benefit, but the service provider receives an endless flood of details *which they can correlate with activity on other web sites using their service*.

Concealment of Activity:

The efforts required to conceal one's activities are nontrivial. Employing the Tor anonymizing network[6] is proof against most attribution efforts up to the nation state level, but its utility for fraudsters makes it unwelcome all over. There is a well known member of the hacker group Anonymous who publishes a guide for accomplishing this. The material is technically demanding the guide is frequently marked incomplete, due to the evolving requirements social media sites employ in order to screen out bots.

Virtual Private Networks[7] are another option for shielding one's location. They are much less likely to be on a web site's proscribed visitors list, but a novice at covert activity will make mistakes like signing up for a service from the public IP of their home service using the same browser that has all the rest of their activity. One can not treat a VPN service like Harry Potter's clock of invisibility, donning it for the sake of subterfuge, then tucking it away when not needed. A skilled operator would build a virtual machine using a hypervisor like VirtualBox or Vmware, configure it to run with a "fail closed" VPN connection, then build the accounts of the persona using a burner phone purchased with cash. Work like this gets done at a coffee shop one does not frequent and the burner phone is turned off before leaving, never to be powered on again.

Those who genuinely need to move without a trace either have the network engineer skill set to the level of being able to capture and analyze traffic, or they pay for a "misattrib" service that handles the technical tradecraft for them.

Attribution of Harassment:

When an unskilled online operator becomes enough of a nuisance that professional assistance is required, there are a few simple steps that always occur.

- Summarize known information such as email addresses, phone numbers, and any social media.
- Employ various free OSINT (Open Source Intelligence) tools to locate any public trails.
- Arrange for the perpetrator to access a web site with basic reporting capabilities such as Google Analytics, or to encounter what the industry calls a canary token.

There are powerful search and correlation tools, some of which are paid and some of which are classified as OSINT, short for open source intelligence. A search across the breadth of all social media platforms for a specific name can be accomplished by a variety of means. There are free to use tools

---

[6]https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser
[7]https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

like Rapportive that will provide background if presented with an email address. There are many poor quality sites offering information on phone numbers, but a skilled operator can usually compare a couple of them and sort out which ones have legitimate information.

There are services that exist specifically to provide a transparent tracking pixels. The content creator for a web site can embed a link to a specific, complex DNS name, tying it to an inconsequential element in a web page. Every site visitor encounters this link and the IP addresses of visitors accumulate in the logs of the service provider.

There are services that provide what are known as a canary tokens, a sort of tripwire alarm for the internet age. These can be a DNS name, an email address, or an object to embed in a document. They don't always get an IP address, but they will show the time of an event and the DNS server that made the request. This serves to narrow searching in a web server's logs.

ADINT[8], short for advertising intelligence, is another hazard. An expenditure of just $100 can reveal all sorts of information about an investigation target.

A Historial Analogy:

When you initiate a phone call the setup involves the destination DNIS (dialed number indication string) and an ANI (automatic number identification). Caller ID began as a value add service for old fashioned analog phone lines. The first ring ensures there is a phone at the far end, then the caller ID data is transmitted as modem tones between the first and second ring. Business phone systems with more than half a dozen lines typically have a digital connection to the phone company rather than a bundle of analog lines. Digital lines mean the DNIS and ANI are simply passed through, making them easily available in the system, even if a caller is feeling clever and pressed *69 prior to dialing.

A caller with some phone system knowledge and access to digital trunks would be able to make a call with less chance of leaving a trail. There are commercial services such as SpoofCard that make this available to the masses. However, if the target is sufficiently motivated, the SS7 system used by phone companies to connect calls keeps records similar to those available for DNS.

Calling, like browsing, might feel safe in one's own home, but there are always trails that are left in the underlying systems.

Conclusion:

Federal statutes on wire taps are found in Title 18 Chapter 119. These laws uniformly address a third party attempting to intercept private communications between others, specifically voice, email, and other person to person methods. None of these laws provide any protection for an unwary nuisance actor visting a monitored site. Some states require two party consent for recording calls, while others are more permissive. None of those laws are applicable, either directly or in spirit, to obtaining the IP address of a nuisance actor by examining data from web browsing activity.

---

[8]https://adint.cs.washington.edu/ADINT.pdf

EXHIBIT B

Shawn Kasal
Digital Forensic Expert
Consulting Engineer & Network Security Consultant
Omaha, Nebraska

Professional Experience

Systems Architect, Systems Engineer, IT Managed Services, Security Consulting
Data forensics & Electronic discovery and Data Recovery Specialist
CJA Expert Panel Federal Public Defenders Offices
Federal Expert Witness - Digital Forensics
Qualified Expert Witness, Digital Forensics under Military Rules of Evidence (MRE)
Subject Matter Expert Network Threat Attribution & Remediation
Special Master: SEC panel FINRA appointment
Privately Retained to investigate network breaches, computer systems abuse, electronic fraud, and intellectual property theft.

Teaching Experience

Returning Guest Lecturer DFIR/SIGINT/OSINT/Diplomatic Digital Security, Institute of World Politics IWP.edu
Adjunct Instructor, Digital Forensics & Cybersecurity, University of Nebraska Kearney, UNK.edu
Cyber Camp Instructor UNK.edu, NSA funded by INQTEL
Law Enforcement only/restricted Digital Forensics Training as Co-Instructor, University of Nebraska Kearney, UNK.edu

Presentations

Nebraska State Bar Association 2019 Annual Meeting, Nebraska Criminal Defense Attorney's Association Seminar: "Digital Forensics: Context and Correlation"

Nebraska Association of Licensed Private Investigators, First Quarter Meeting 2020, "Forensics for Private Investigators"

Kutak Rock Special Guest Speaker: "Digital Forensics in Legal Investigations"

Training and Certifications

CompTIA A+ Linux+ Network+ Security+ Server+

Microsoft MCP NT 4 MCSE for Windows 2000, 2003, 2008, 2012

Network attribution on Darknets (tor) (p2p) (VPN) (other network obfuscation methods)

Compliance and Security Auditing PCI, HIPAA

EC-Council's Certified Ethical Hacker (CEH) v8 courseware training

Cellebrite Advanced Smartphone Analysis training

CCDA (Cisco Certified Design Associate)

CCNA (Cisco Certified Network Analyst) - Security

CCNP (Cisco Certified Network Professional) - Wireless

CCNP (Cisco Certified Network Professional) - Routing and Switching

Business and Organizations served

(NC4) CyberCop Consultant and Intel Analyst

US Air Force 16 AF/JA (Digital Forensic Expert for Prosecution and Defense trial counsel)

Ankura Consulting, Washington DC as Contractor (Digital Forensics and Incident Response support including OSINT mapping of Geo-political threats and Due Diligence Risk Mitigation in Merger and Acquisitions)

Kutak Rock, Nebraska, Arkansas, (Digital Forensics and Incident Response and Expert Witness)

Koley Jessen, Nebraska, (Digital Forensics and Incident Response and Expert Witness)

D4 Discovery (Special Counsel) as Contractor (Digital Forensics and Incident Response and E-Discovery, Data collections specialist)

Avalon Cyber as Contractor (Digital Forensics and Incident Response and E-Discovery, Data collections specialist)

Federal Public Defenders Office - Omaha, NE, Des Moines, IA, Tacoma, WA, Rochester, NY (appointed and privately retained as Digital Forensics Expert Witness)

Public Defenders Offices in Sarpy County, Oto County, Hall County, NE, Polk County, IA (Digital Forensics Investigator and Expert Witness)

General Motors (network security consultant and incident response)

Ford Motor Corporation (network security consultant)

Daimler Benz (network security consultant)

Sid Dillon Chevrolet Buick GMC Cadillac Mazda Nissan Hyundai (Systems Engineer)

Dillon Brother's Harley-Davidson (Systems Engineer)

Plaza Buick GMC (Systems Engineer)

Woodhouse Auto Group (Consulting Systems Engineer)

Wicks Truck Trailers (Systems Engineer)

Forensic Tools and Software Qualifications

Cell Hawk: Hawk Analytics PCMD CDR data Geo-Locational Analysis of Subscriber Data
SANS Digital Forensics Incident Response: Advanced Smart Phone Forensics.
SANS webinar training Volatility memory forensics tool and methods.
Cellebrite (UFED) Universal Forensics Extraction Device and related software.
MOBLedit Forensic Capture Methodology
SANS Investigative Forensic Toolkit (SIFT)
Access Data's Forensic Tool Kit (FTK)
HP MicroFocus's ArcSight Logger.
Guidance Software's EnCase Forensics
BlackBag's Mobilyze (mobile phone forensics)
BlackBag's Macquisition Mac OS drive acquisition tool
BlackBag's BlackLight Mac OS and Microsoft Windows forensic toolkit
White Glove Linux by Dr. Fred Cohen
CAINE (Computer Aided Investigative Environment)
HELIX3 is a live CD-based digital forensic suite
SleuthKit's Autopsy – Open Source Digital Forensics
Katana Forensics (Linux) and Lantern (Mac)
PassMark's OSForensics (PC) Windows
Paraben's P2X forensic mount tool & E3DS mobile device tool
X-Ways Forensics, WinHex
Email Investigations (MS Exchange and Unix MTA's)
Security Information and Event Management (SIEM) solutions like: AlienVault: Splunk: Security Onion, Wazuh
Open Source Intelligence Techniques (OSINT)
Basic Investigations of Windows Unix and Mac
InDepth Investigations of Windows Unix and Mac
Reverse Engineering Malware (NIT)
MetaSploit by Rapid7
Nessus Security Scanner by Tenable.

Investigating Linux from a Forensic and Incident Response Perspective
MySpace, Facebook, Twitter, Tumblr Investigations
Cyber child Exploitation - Investigations in the Workplace
Grindr, Snapchat, Tinder, other similar mobile chat apps
Digital Forensics Framework -Unix
Open Computer Forensics Architecture (OCFA)
Xplico is an open source network forensic analysis tool
Volatility is the memory forensics framework
Oxygen Forensic Suite
Computer Online Forensic Evidence Extractor or COFEE is a tool kit developed for computer forensic experts by Microsoft
Case Study Firefox, Google Chrome Artifacts and Unallocated Space
Technical Profiling for Intelligence (metadata foot printing) Profile online identity
Malicious Artifacts Identification and Analysis
Essential Macintosh Forensics Mac OS X 10 to 10.13
IOS Forensics – A comprehensive Approach
Android Forensics - A Comprehensive Approach